

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

598 Dreese Laboratory 2015 Neil Ave., Columbus, Ohio
43210
(OFFICE PREMISES)

Case No. 2:21-mj-694

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See attached Affidavit in support of this Application, and Attachment A-3 thereto, all of which is incorporated herein by reference.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See attached Affidavit in support of this Application, and Attachment B thereto, all of which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. 1343
18 U.S.C. 1001

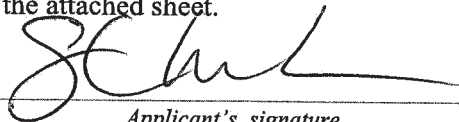
Wire Fraud
False Statements

Offense Description

The application is based on these facts:

See attached Affidavit incorporated herein by reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature


Steve McCann, SA FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: October 27, 2021

City and state: Columbus, Ohio


 Kimberly A. Tolson
 United States Magistrate Judge



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**IN THE MATTER OF AN
APPLICATION FOR A SEARCH
WARRANT FOR THE PREMISES
KNOWN AND DESCRIBED AS:**

- **10309 MacKenzie Way, Dublin, Ohio 43017 (HOME/COMPANY PREMISES)**
- **578 Dreese Laboratory 2015 Neil Ave., Columbus, Ohio 43210 (LAB PREMISES)**
- **598 Dreese Laboratory 2015 Neil Ave., Columbus, Ohio 43210 (OFFICE PREMISES)**

Case No. 2:21-mj-694

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Steve McCann, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. As set forth in detail below, federal law enforcement is conducting an investigation into possible violations of federal criminal laws by Deliang WANG (WANG). In particular, Your Affiant submits that the facts herein establish probable cause to believe WANG has committed violations of 18 U.S.C. § 1001 (False Statements), and 18 U.S.C. § 1343 (Wire Fraud) (collectively referred to as the SUBJECT OFFENSES).

2. Relevant here, I make this Affidavit in support of an Application for a search warrant to search the premises known and described as: (1) 10309 MacKenzie Way, Dublin, Ohio 43017 (the "HOME/COMPANY PREMISES"); (2) 578 Dreese Laboratory 2015 Neil Ave., Columbus, Ohio 43210 (the "LAB PREMISES") and (3) 598 Dreese Laboratory 2015 Neil Ave., Columbus, Ohio 43210 (the "OFFICE PREMISES") (together referred to as the "SUBJECT

PREMISES”), further described in Attachments A-1, A-2, and A-3; and to seize the things described in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES will be found within the SUBJECT PREMISES.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. AGENT BACKGROUND

4. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since March 2008, and I am currently assigned to the Cincinnati Division, Columbus Resident Agency, as a member of the Counterintelligence Squad. I am responsible for investigating, among other crimes, false statements and wire fraud. I have received both formal and informal training in the detection and investigation of said offense. As a result of my training and experience, I am familiar with the federal laws relating to the SUBJECT OFFENSES. As a federal agent, I am authorized to investigate violations of the laws of the United States.

5. I am currently involved in a joint criminal investigation of Deliang WANG. Along with my co-case agents from the FBI and the Office of Inspector General for the United States Department of Health and Human Services, I have personally participated in the investigation described herein. I have reviewed any relevant documents and reports of witness interviews during the course of this investigation. The statements contained in this Affidavit are based on my own observations, document reviews, and reliable information provided to me by other law enforcement officials. Because this Affidavit is being submitted for the limited purpose of establishing probable cause to search the property described below, I have not included each and every fact learned during the course of this investigation. Rather, I have set forth those facts that I believe are necessary to establish probable cause for the search warrant sought. Where actions,

conversations, and statements of others are related, they are related in part, except where otherwise indicated.

6. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that violations of the SUBJECT OFFENSES have been committed by WANG. There is also probable cause to believe that fruits, evidence, and instrumentalities of these crimes, as described in Attachment B, are located at the SUBJECT PREMISES, as described in Attachments A-1, A-2, and A-3.

III. JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

IV. APPLICABLE STATUTES AND DEFINITIONS

8. I am advised that:

9. Title 18, United States Code, Section 1001(a) provides, in relevant part, that “whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact” or “makes any materially false, fictitious, or fraudulent statement or representation” is in violation of federal law.

10. Your Affiant is also advised that U.S. law prohibits the use of an interstate telephone call or electronic communication made in furtherance of a scheme to defraud. Title 18, United States Code, Section 1343 provides, in relevant part, that “whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means

of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice” is in violation of federal law.

V. PRIOR APPLICATIONS

11. On or about February 10, 2020, an email search warrant on WANG’s GMAIL email account (pnlwang@gmail.com), signed by U.S. Magistrate Judge Kimberly A. Jolson, was issued in the Southern District of Ohio.

12. On or about May 8, 2020, an email search warrant on WANG’s GMAIL and Ping BAI’s (WANG’s wife) GMAIL email accounts (pnlwang@gmail.com and bailingosu@gmail.com respectively), signed by U.S. Magistrate Judge Elizabeth A. Preston Deavers, was issued in the Southern District of Ohio.

13. On or about March 24, 2021, an email search warrant on WANG’s OSU email account (dwang@cse.ohio-state.edu), signed by U.S. Magistrate Judge Elizabeth A. Preston Deavers, was issued in the Southern District of Ohio.

VI. INVESTIGATION AND PROBABLE CAUSE

A. Deliang WANG

14. WANG has been an employee of OSU since 1991. WANG is currently a professor in OSU’s Department of Computer Science and Engineering, as well as in OSU’s Center for Cognitive and Brain Sciences. Additionally, WANG is a faculty member of the OSU Laboratory for Artificial Intelligence (AI) Research. WANG also serves as the Director of the OSU Perception and Neurodynamics Lab (PNL). WANG’s lab conducts research regarding a variety of topics under the general theme of computational audition, including speech separation and robust

automatic speech/speaker recognition. (Your Affiant is advised that computational audition concerns the study of how the human brain processes sound and speech, and how the brain's processing of this sensory input can then be transferred to machine learning.)

15. AI has been defined as the theory and development of computer systems to be able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

B. Conflict of Interest Reporting Requirements

16. Based upon information obtained from OSU's Faculty Financial Conflict of Interest (COI) Policy dated February 5, 2013, "a conflict of interest exists if financial interests or other opportunities for tangible personal benefit may exert a substantial and improper influence upon a faculty member or administrator's professional judgement in exercising any institutional responsibility." (Based on the facts laid out in this Affidavit, WANG's undisclosed conflicts related to his NIH grants began to arise in at least 2015; therefore, the above policy was the operative policy in place during the time periods relevant to this Affidavit. OSU since updated its COI policies in 2017, only to be more restrictive on reporting of COIs.) "Financial interest," as defined by OSU's Faculty Financial COI Policy, dated February 5, 2013, is any equity interest held in a non-publicly traded entity, or more than \$10,000 in income from a publicly or non-publicly traded entity received during a 12-month period.

17. OSU policy requires conflicts of interest to be filed annually. Updates must be made to the disclosure within thirty (30) days of the filing party acquiring any new financial interests, external professional activities, or business or financial transactions that were previously unreported, or if changes occur in the circumstances of a previously reported transaction or activity.

18. As further described in this document, some of WANG's AI research at OSU is funded by grants from the federal government, specifically the U.S. National Institutes of Health (NIH).

19. Federal COI regulations, as well as OSU policy, require researchers to update their COI disclosures within 30 days of receiving any new financial interest with an outside entity, or within 30 days of any changes to a currently disclosed financial interest. In particular, this includes any interest in a company, business, foundation, or other organization that: provides products or services in one's academic or research discipline; could make use of one's scholarly work or research either directly or indirectly; could reasonably appear to impact one's research or other obligations. These COI regulations also require disclosure if one receives royalties directly from intellectual property that one has licensed to an external entity.

20. Additionally, NIH has a policy concerning patents being disclosed to NIH. NIH's policy requires action before a grant recipient participates in NIH-funded research and development: "Recipient employees [here, WANG] working under a federal funding award (other than clerical and nontechnical employees) must sign an agreement with the recipient organization [here, OSU]. This agreement requires the Recipient employee to: (1) disclose promptly in writing to personnel identified as responsible for the administration of patent matters each Subject Invention made under NIH funding; (2) assign to the Recipient [i.e., OSU] the entire right, title and interest in and to each Subject Invention made under the funding agreement; (3) execute all papers necessary to file patent applications on Subject Inventions; and, (4) establish the government's right in the Subject Inventions." Furthermore, NIH policy states that the recipient of NIH funding must submit to NIH a disclosure for all Subject Inventions. (As defined by 37

CFR 401(a)(2), “subject invention means any invention of the contractor conceived or first actually reduced to practice in the performance of work under this contract.”)

C. 18 U.S.C. § 1001 Relating to Grant Applications, Conflict of Interest Filings, and NIH Progress Reports

21. On or about March 1, 2012, an NIH grant utilizing form SF 424 (R&R), Application for Federal Assistance, was submitted and listed WANG as the Principal Investigator (PI). The proposed project dates were October 1, 2012, through September 30, 2017. The amount of funding requested for this application was \$1,791,142. The title of the grant application was “Speech segregation to improve intelligibility of noisy speech.” Through this application, WANG was awarded NIH grant number 1 R01 DC012048.

22. On or about February 28, 2017, a renewal application for further Federal Assistance under NIH grant number 1 R01 DC012048, with proposed project dates of October 1, 2017, through September 30, 2022, was submitted, with a proposed projected funding of \$1,775,727.

23. As of February 23, 2021, a total of \$2,320,429.02 has been authorized for grant number 1 R01 DC0125048.

24. Your Affiant understands NIH policy mandates that NIH-funded researchers disclose outside financial interests to their employing entity (in WANG’s case, OSU), either at the time of application, annually, or within 30 days of acquiring such financial interest. The employing entity then discloses this information to NIH.

25. The NIH grant submission form, SF 424 (R&R), Application for Federal Assistance, states: “By signing this application, I certify (1) to the statements contained in the list of certifications* and (2) that the statements herein are true, complete and accurate to the best of my knowledge. I also provide the required assurances * and agree to comply with any resulting terms if I accept an award. I am aware that any false, fictitious or fraudulent statements or claims may

subject me to criminal, civil, or administrative penalties. (U.S. Code, Title 18, Section 1001).” Your Affiant notes this to show WANG’s knowledge of the statute as it relates to his NIH funding application, and his knowledge about the importance of telling the truth when seeking large amounts of federal funds.

26. WANG also submitted Research Performance Progress Reports (RPPR) to NIH from 2013–2020. According to NIH’s website, “[t]he RPPR is used by grantees to submit progress reports to NIH on their grant awards.”

27. Relevant to WANG’s false statements via wire, WANG submitted to NIH at least four RPPRs after July 20, 2017:

| | <u>Date of Submission</u> | <u>RPPR Number</u> | <u>Reporting Period</u> |
|----|---------------------------|----------------------------------|-------------------------|
| 1. | 04/23/2018 | 5 R01 DC012048-05 RPPR (interim) | 01/01/2017 – 01/09/2018 |
| 2. | 11/13/2018 | 5 R01 DC012048-07 RPPR | 01/08/2018 – 12/31/2018 |
| 3. | 11/05/2019 | 5 R01 DC012048-08 RPPR | 01/01/2019 – 12/31/2019 |
| 4. | 11/05/2020 | 5 R01 DC012048-09 RPPR | 01/01/2020 – 12/31/2020 |

28. The investigation has indicated that WANG filled out the above RPPR documents in preparation for a nominal “signing official” from OSU to sign prior to their submission to NIH. WANG submitted the documents electronically, in the process of which he clicked on a screen to acknowledge his acceptance of the following NIH “Assurance Statement”: “I certify that the statements herein are true, complete and accurate to the best of my knowledge. I am aware that any false, fictitious, or fraudulent statements or claims may subject me to criminal, civil, or administrative penalties. As PD/PI, I agree to accept responsibility for the scientific conduct of the project and to provide the required progress reports if a grant is awarded as a result of this submission.”

29. In other words, each time WANG routed an RPPR to a nominal signing official at OSU, WANG gave assurances that he was making true, complete and accurate statements and was aware of the criminal penalties for not being truthful. According to information provided by NIH, WANG clicked to accept this “Assurance Statement” 11 times from 2013 to present.

30. Additionally, the investigation has discovered that WANG’s below-described materially false reports were committed via wire, in violation of 18 U.S.C. § 1343. According to information obtained from NIH Extramural Research Integrity Office (NIH-ERIO), WANG routed the RPPRs to OSU for submission by logging into NIH systems, via the internet, while using his log-in ID to route the reports.

1. Failure to Disclose Conflicts of Interest

31. Each RPPR provides the researcher an opportunity for disclosure of other financial support. For instance, Section D.22.c of the RPPR seeks information on “Changes in Other Support.” This is an almost yearly opportunity, along with the previously mentioned Conflict of Interest reporting previously mentioned, to make disclosures to NIH.

32. According to open-source information, WANG was the co-founder and chief scientist at a company called ELEVOC. According to ELEVOC’s LinkedIn profile, ELEVOC was established in 2015 and is now based in Shenzhen, China. ELEVOC’s work is focused on the application development of deep learning in the field of speech enhancement and signal processing technology. On ELEVOC’s web page, WANG is cited as the first person in the world to apply deep learning to speech enhancement.

33. Open-source research conducted on or about May 9, 2019, revealed that on July 10, 2018, ELEVOC announced that it received an investment of tens of millions of Renminbi (RMB) from XIAOMI and QUALCOMM. Around that time, as of November 18, 2019, one RMB was

equivalent to .14 United States Dollars. Cui Baoqiu, chief architect of XIAOMI and vice president of the artificial intelligence and cloud platform, said: "In view of the deep application of AI in voice and other fields, AI will be one of the most important strategies for Xiaomi in the next decade. The technical team of Elephant Sound (also known as ELEVOC) is based on many years (of experience). The research and accumulation of computational auditory scene analysis will definitely bring more exciting human-computer interaction experience to the next generation series of intelligent voice products of Xiaomi and Xiaomi Ecological Chain."

34. According to the Ohio Secretary of State website, WANG and his wife, Ping BAI, registered a company in Ohio called MACHINE PERCEPTION CO on or about March 10, 2014. WANG is listed as the Agent/Registrant of MACHINE PERCEPTION. WANG updated MACHINE PERCEPTION's registration through electronic filing on June 4, 2018. MACHINE PERCEPTION was registered at 10309 MacKenzie Way, Dublin, Ohio 43017, the HOME/COMPANY PREMISES.

35. ELEVOX is a company incorporated in the State of Delaware on November 9, 2015. According to ELEVOX's Annual Franchise Tax Report, discovered during a review of search warrant results concerning WANG's Gmail account, WANG and Jianzhang MIAO were listed as the Directors of ELEVOX. Based upon its bank statements, ELEVOX acts as a shell company that accepts money funneled from ELEVOC, a Chinese company, through ELEVOX, then to accounts associated with MACHINE PERCEPTION, and finally on to personal accounts to which WANG has control or access.

36. Additionally, ELEVOX's listed place of business on the aforementioned tax report was the HOME/COMPANY PREMISES, 10309 MacKenzie Way, Dublin, Ohio 43017. This investigation has shown that this is also WANG's home address.

37. ELEVOC, ELEVOX, and MACHINE PERCEPTION were founded while WANG was an employee of OSU. Per the terms of receiving NIH grant money, and per the terms of the COI requirements at OSU, WANG was required to disclose to OSU, and then to NIH, his other financial Conflicts of Interest—including, for example, his involvement with ELEVOX, ELEVOC, and MACHINE PERCEPTION.

38. Of these companies, ELEVOX is the only company WANG has disclosed to OSU, though his disclosure was neither timely nor complete. WANG disclosed to OSU his ownership in ELEVOX (the American-based shell company that appears to exist to move money from China to the United States)—not ELEVOC (the China-based company that actually engages in AI-related business)—on or about May 15, 2017, *after* the submission of his NIH grant renewal. In his disclosure to OSU, WANG stated he was paid a maximum of \$59,998 and his ownership in the company was estimated as \$250,000 or more. ELEVOX was incorporated on or about November 9, 2015, in the State of Delaware. WANG's disclosure of ELEVOX to OSU shows he was aware of the procedures to disclose a potential conflict of interest.

39. The investigation has demonstrated that WANG used ELEVOX to funnel money from ELEVOC, WANG's Chinese company, to MACHINE PERCEPTION, WANG's Ohio-based company. Specifically, between approximately May of 2017 to approximately January of 2020, \$330,000 has been wired from ELEVOC (in China) to the ELEVOX account in the United States. From there, the investigation indicates that WANG has diverted a significant portion of those incoming funds to MACHINE PERCEPTION, and then on to various additional accounts in WANG's name or control.

40. In my training and experience, I have come to understand that university researchers with ties to undisclosed companies conducting research/work similar to what the

researchers are doing at their university creates a potential conflict of interest. Such undisclosed companies are a way for researchers to illegally profit from intellectual property developed at the university and funded by U.S. Government grants. As referenced above, OSU and NIH both have policies in place to enable researchers to disclose and mitigate conflicts of interest related to work conducted using NIH funds and/or University resources.

2. False Statements: Patents

41. As to each RPPR, there is probable cause to believe that WANG provided and affirmed false statements concerning the patents that he held in China. Under section C.4 of each of the RPPRs, titled "INVENTIONS, PATENT APPLICATIONS, AND/OR LICENSES," WANG was asked, "Have inventions, patent applications and/or licenses resulted from the award during the reporting period?" WANG answered "No."

42. As described below, this response was in direct violation of 18 U.S.C. § 1001.

43. Open-source information and information obtained from OSU indicate that ELEVO, WANG's company in China, has filed eight patents in China with topics closely related to WANG's AI research at OSU. For example, the patents pertain to, among other topics, AI-related speech enhancement and noise reduction, both of which were the subject of WANG's research and development of proprietary information and technology at and on behalf of OSU utilizing NIH funds. On some of these patents, the inventor(s) waived the right to be mentioned. WANG is listed as an inventor of patent CN107452389A, further described in the table below. These patents were also required, per NIH policy, to be disclosed to NIH. To date, WANG has not disclosed the existence of any of the eight patents, or his relationship to them, to OSU or NIH.

44. The patent numbers, dates the patent applications were filed, and the titles of the aforementioned Chinese patents are listed below:

| Patent Number | Date Application was Filed/Title | Inventor |
|----------------------|--|---|
| CN107452389A | 07/20/2017. A kind of general monophonic real-time noise-reducing method | Jitong CHEN (Ph.D. from OSU under WANG 2017), Xueliang ZHANG (Visiting scholar at OSU from 2013-2014; Postdoctoral researcher for WANG at OSU from 2014-2016; Recruited by WANG for Northwestern Polytechnical University's Thousand Talent Program 2016), Deliang WANG |
| CN109839612A | 08/31/2018. Sound source direction estimation method based on time-frequency masking and deep neural network | Waived right to be mentioned. |
| CN109841206A | 08/31/2018. A kind of echo cancel method based on deep learning | Waived right to be mentioned. |
| CN109841226A | 08/31/2018. A kind of single channel real-time noise-reducing method based on convolution recurrent neural network | Waived right to be mentioned. |
| CN110265020A | 07/12/2019. Voice awakening method, device and electronic equipment, storage medium | Xiang Duan, Zhenbin Zhang |
| CN110660406A | 09/30/2019. Real-time voice noise reduction method of double-microphone mobile phone in close-range conversation scene | Ke TAN (Research Associate at OSU 2017-present; Research Intern at ELEVO Apr. '18, May '18 and Dec. '18-Jan '19), Yongjie YAN |
| CN110767223A | 09/30/2019. Voice keyword real-time detection method of single sound track robustness | Peng HU, Yongjie YAN |
| CN110931031A | 10/09/2019. Deep learning voice extraction and noise reduction m...sing bone vibration sensor and microphone signals | Yongjie YAN |

45. As previously mentioned, WANG affirmed via multiple RPPR submissions, and subject to criminal penalty, that no “inventions, patent applications and/or licenses resulted from the award during the reporting period” related to various NIH grants for which WANG has

received funding. Relevant to the SUBJECT OFFENSES, WANG made these affirmations via NIH's online portal on or about April 22, 2018, November 11, 2018, November 5, 2019, and November 5, 2020.

46. In conducting its own diligence regarding these patents, OSU commissioned an expert analysis of three of the eight Chinese patents (CN107452389A, CN109839612A, and CN109841206A) and how they relate to WANG's research at OSU. According to that review, "(p)reliminary analysis suggests that U.S. government funding led to discoveries that are included in patent claims within some of the selected patents." The expert analysis further stated: "Of the three patents analyzed in this report, all show significant similarity or overlap with published manuscripts that cite federal funding. While some similarities in technical publications or communications can naturally occur if the works build on a common work that was published earlier, the level of similarity in the analysis above goes far beyond that which would be expected of normal research progression. The analysis in this report suggests very strong borrowing or copying of technical ideas, algorithms, and experimental setups from one set of published works to the patents that were analyzed."

47. On ELEVOC's Chinese Patent CN109841206A, the inventor declined to be listed. The patent was filed on August 31, 2018. OSU identified two subsequent WANG publications that contained substantially similar content to this patent. Both were published in or around September of 2019. Accordingly, there is probable cause to believe that WANG used unpublished research conducted at OSU with NIH funds to apply for ELEVOC's Chinese patent.

D. Wire Fraud: For-Profit, External Contracts between ELEVOC and LENOVO China

48. According to open-source internet sources, Lenovo is a multinational technology company incorporated in Hong Kong that also global headquarters in Beijing, China, operational

headquarters in Morrisville, North Carolina, and an operational center in Singapore. Lenovo produces various computer hardware devices such as laptops, personal computers, tablets and smartphones. The company has operations in over sixty (60) countries and sells its products in approximately one-hundred-and-eighty (180) countries.

49. Based upon the investigation, law enforcement has identified relevant documentation regarding WANG's, and ELEVOC's, business relationship with Lenovo. This documentation included: contracts between an overseas entity (Lenovo China) and ELEVOC, as well as relevant attachments and/or amendments; an email chain that was forwarded to Lenovo's Director of Software Procurement in the United States, which included negotiations with ELEVOC regarding one of the amendments; and three additional emails in the possession of Lenovo's Director of Software Procurement that appear to be responses from ELEVOC to a Request for Quote/Proposal.

50. An analysis of the above-named documents determined Lenovo China entered into a "Software License and Distribution Agreement" (hereinafter 'contract') with Elevoc Technology Co., LTD., Guadong, China (IE Deliang Wang). The original contract agreement is dated 12/11/2019. The contract contains sealed stamps affixed to the document by both Lenovo and ELEVOC. The agreement indicates it was finalized on July 2, 2020. Based on this information, Lenovo China entered into a contract with ELEVOC to purchase or license software products.

51. According to language in the original contract, the contract grants Lenovo world-wide distribution rights (via its various hardware products sold to end users) of specified ELEVOC software. Based upon the documentation and contracts between ELEVOC and Lenovo, the business arrangement centered on Lenovo using ELEVOC software related to the following: noise suppression, VOIP noise suppression, and noise suppression for recording.

52. The contractual agreement between Lenovo and ELEVOC further outlined fees and royalties related to the software at issue. Your Affiant understands that the contractual agreement, as well as other documents related to the Lenovo–ELEVOC business relationship, indicate the following:

- a. That Lenovo was to be paid a one-off licensing fee related to the VocplusTablet software of approximately \$57,750.00; and
- b. That, based upon royalty figures associated with the Vocplus Tablet software and upon sales-figure projections associated with the software, ELEVOC was projected to make at least \$700,000 based on the parties' agreement.

53. Moreover, sales records from Lenovo regarding the contracts at issue that ELEVOC in fact was paid at least \$230,000 related to the parties' contract.

54. Your Affiant notes that Chinese patent number CN107452389A, titled, "A kind of general monophonic real-time noise-reducing method," bears a close similarity to the work on the contract described in the LENOVO contract referenced above. As previously noted in this document, this is the same Chinese patent obtained by WANG for ELEVOC that was similar to or overlapped with published manuscripts that, according to the manuscripts, related to research derived from federal funding.

55. Per the terms of WANG's employment with OSU, OSU retains the rights to any of WANG's inventions relating to his employment with OSU. Moreover, per the terms of OSU's COI requirements, WANG was required to disclose to OSU the existence of his outside business interests with Lenovo, as well as his use of OSU- and NIH-related research in furtherance of his outside business interests with Lenovo. Moreover, NIH's COI regulations also required WANG to disclose to OSU the existence of any patents related to NIH-funded research.

56. The investigation has indicated a high likelihood that the intellectual property underlying ELEVOC's contracts and business arrangement with Lenovo was substantially similar to, and likely derived from, NIH-funded research WANG performed at OSU.

57. To date, the investigation has indicated that WANG did not disclose the following to OSU or NIH: ELEVOC; the extent of ELEVOC's business in China; ELEVOC's and WANG's business relationship with Lenovo; the use of NIH-related research and intellectual property in the context of ELEVOC's and WANG's business relationship with Lenovo.

58. Based upon these facts and Your Affiant's training and experience, Your Affiant has probable cause to believe the following: while failing to make the disclosures just described, WANG has used U.S. government funding and OSU intellectual property to create patents in China under his company ELEVOC and is using the technology or the derivative of that technology for personal gain in the aforementioned contractual agreement between ELEVOC and Lenovo, all in violation of 18 U.S.C. § 1343.

E. Additional Relevant Information: WANG'S Thousand Talents Plan Participation

59. WANG has engaged in additional conduct that is relevant to his misstatements in violation of 18 U.S.C. § 1001, and his intent to defraud in violation of 18 U.S.C. § 1343.

1. WANG's Misstatements Regarding His Thousand Talent Plan Participation

60. In addition to his work at OSU, WANG has conducted work with and for various institutions in China. According to an article about WANG located on a website run by the Hexian government (www.hx.gov.cn), in 2017 WANG was cited for his accomplishments and contributions to China. The article stated in relevant part: "Wang Deliang loves the motherland and often returns to China to give lectures. He has lectured at Beijing University, Tsinghua

University, the University of Science and Technology of China, Shanghai Jiao Tong University, and other universities and there is none of his own research which he has not retained and presented to the motherland.”

61. The investigation has shown that WANG has been engaged as a Thousand Talents Plan member during the course of receiving money from NIH. Based on my training, experience, Your Affiant is aware that the Thousand Talents Plan aims to recruit overseas scientists, engineers, and other experts to work for businesses, research institutes, and government agencies in China, with the goal of utilizing these experts to further the PRC Government’s strategic national development goals. Your Affiant is further aware that recruits of Thousand Talents Plans typically sign contracts that detail the specific research they will perform or the business they will develop in China. That contractual obligation often resembles or even replicates the work the recruit performs or performed for his or her U.S.-based or other overseas employer, thereby leveraging the recruit’s knowledge and access to intellectual property obtained from U.S. and foreign businesses, government laboratories, and research institutions.

62. Open-source information reviewed on or about July 5, 2019, revealed WANG was among the tenth batch (2014) of the Thousand Talent Program (TTP) of the Organization Department of the Central Committee of the Chinese Communist Party, and his work was in the area of machine perception and signals processing. WANG’s TTP position was at Northwestern Polytechnic University’s (NPU) Center for Intelligent Acoustics and Immersive Communications (CIAIC). WANG listed on his biographical sketch, associated with the 2017 renewal NIH grant renewal application, that he was employed in 2015 as a Visiting Scholar at NPU in the CIAIC. (NPU was added to the U.S. Department of Commerce’s Designated Entity List in or around September 2012. The Entity List identifies entities and other persons reasonably believed to be

involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.)

63. Based upon WANG's 2019-2023 employment contract, his TTP position at NPU required that WANG: work to cultivate graduate students; teach a course sponsored National Natural Science Foundation of China (NNSFC); teach courses regarding AI-related technology; refer 2–3 candidates per year for state level talent plans such as the TTP; recruit or cultivate 2–3 state level high caliber talents; and lead the PRC's National Defense Key Lab's "Underwater Information Processing and Control" team in its signal processing R&D work, such as underwater voice communication, target detection and channel estimation.

64. Further relevant to this Affidavit, WANG was selected for a TTP position at NPU in 2014, and accordingly began his work with the program in January of 2015.

65. On or about February 28, 2017, WANG submitted a renewal application for Federal Assistance from NIH with proposed project dates of October 1, 2017, through September 30, 2022, with projected funding of \$1,775,727.

66. On WANG's February 28, 2017 NIH renewal application, while disclosing his association with NPU as a Visiting Scholar in his biographical sketch, WANG did not disclose his employment as a TTP member.

67. WANG did not fully disclose his NPU employment to OSU until May 15, 2017. When he did disclose his affiliation with NPU, WANG represented the affiliation had no teaching involvement. WANG also represented that it was "unknown" regarding the position being a Talent Program position. Instead, WANG represented his affiliation with NPU as personal consulting.

68. On or around June 26, 2018, WANG disclosed to OSU the full extent of his TTP position at NPU that began on or around January 1, 2015. WANG was advised by OSU after this disclosure that it was in his best interest to resign his position at NPU.

69. Your Affiant has viewed, from Gmail Search Warrant returns, WANG's resignation acceptance letter from NPU dated June 18, 2019, which WANG submitted to OSU. Despite that letter, on or about June 24, 2019, WANG communicated by email with his lab leader at NPU, during which WANG and his lab leader at NPU discussed WANG helping to recruit scholars for NPU's CIAIC. This assistance fell within the TTP responsibilities he had ostensibly relieved himself of by resigning.

2. Still Undisclosed TTP Affiliation

70. According to a document found in WANG's pnlwang@gmail.com email account, listing the date of application as November 5, 2018, WANG applied for the "Talent Rewards for the Thousand Talents Program in Xi'an High-tech Zone." The listed employer for WANG on the document was "Shengeng Intelligent Technology (Xi'an) Research Institute Co., Ltd." (Xi'an Research Institute) and the professional direction listed was machine perception and signal processing. Xi'an Research Institute was established on October 18, 2018, with a registered capital of 6.5 million RMB. The business scope was acoustic sensing, acoustic signal sensing, processing technology, image sensing technology, optical sensor technology, technology development, technical consulting, technical services, technology transfer, etc. On the application, WANG listed himself as being co-founder and Chief Scientist of Elephant Sound (ELEVOC), as well as professor at Northwestern Polytechnical University and Ohio State University. WANG listed his current and past NIH funding as two of the major projects he has led.

71. Also relevant, on or about September 9, 2018, WANG sent a document from his email address stating that he was applying for TTP money with respect to the Xi'an High-tech Zone, and further stating that his intent to use his research to benefit the national development of China.

72. According to open-source research, Xi'an Research Institute is a privately owned institute, established in 2018 by former Bell Lab researcher(s), TTP expert(s) and multiple acoustic experts and scientific research staff. It's located at Area A and Area C on the 12th Floor, Building 5 of Shenzhou Digital Technology Park, No. 20 Zhangbasi Road, Xi'an High-Tech Zone, Xi'an, Shaanxi. The Institute has in-depth collaboration with NPU's CIAIC. The business range of the Institute includes frontier theoretical research and technical development of acoustic signal processing and sensing, arrayed signal processing, speech enhancement processing, acoustic time testing and understanding, machine learning, noise control, acoustic imaging, auditory perception, human factors engineering, distributed optimization, image processing, etc.

73. On a document found in WANG's pnlwang@gmail.com email account, signed by WANG on November 5, 2018, WANG provided his commitment of responsibility for project objectives addressed to the Administrative Committee of [Xi'an] Hi-Tech Industries Development Zone [the Committee] from the Xi'an Research Institute. The document states: "Based on relevant policies under the Committee's Special Talent Crossing Plan for Ten Thousand Talents Plan and Thousand Talents Plan [TTP] selectees, the Company's employee WANG Deliang, a TTP expert introduced by the Committee in 2018, has been awarded for innovation and entrepreneurship in the Hi-Tech Zone."

74. This document also outlines the scope of the commitment between the Xi'an Research Institute and the administrative committee of the TTP committee. Below is a verbatim translation of the communication:

| | 1 st fiscal year (Nov. 2018. 11- Dec.2019) | 2 nd fiscal year (Jan. 2020-Dec. 2020) | 3 rd fiscal year (Jan. 2021-Dec. 2021) |
|--------------------------|---|--|---|
| Completed Investment | RMB two million Yuan | RMB four million Yuan | RMB six million Yuan |
| Project Progress | Product approval and iteration | Small batch production | Mass production |
| Technical Specifications | Technical implementation of multi-channel acquisition of acoustic signals; wave beam forming; echo cancellation; speech noise reduction; dereverberation, de-jamming, positioning, tracking and separation of acoustic source, etc. | Technical implementation of systematic integration of microphone array technology, remote speech technology, acquiring, coding, transmitting and playing high fidelity 3D speech signal, reconstruction of 3D acoustic signals, etc. | Optimization and iteration of system according to the feedback of application in actual scenario. |
| Sales | RMB 1 million Yuan | RMB 3 million Yuan | RMB10 million Yuan |
| Tax | RMB 30,000 Yuan | RMB 90,000 Yuan | RMB 500,000 Yuan |
| Patent Acceptance | Six | Eight | 10 |
| Social Security | 10 people | 25 people | 40 people |

75. A search of Xi'an Research Institute in patentguru.com's database shows Xi'an Research Institute, as of September 22, 2021, holds 17 patents in China.

76. To date, OSU or NIH have not produced any material that has shown WANG has disclosed his TTP award and obligations under the Xi'an High-tech Zone, his employment agreement with Xi'an Research Institute, or his partial ownership of the Xi'an Research Institute.

F. There is probable cause to believe evidence of the SUBJECT OFFENSES will be found in the SUBJECT PREMISES.

77. According to the Ohio Secretary of State website, WANG and his wife Ping BAI registered MACHINE PERCEPTION CO on or about March 10, 2014. WANG is listed as the Agent/Registrant of MACHINE PERCEPTION. WANG updated MACHINE PERCEPTION's registration through electronic filing on June 4, 2018. The listed location of the company was Dublin, Ohio. Additionally, the address listed under the agent/registrator information was 10309 MacKenzie Way, Dublin, Ohio 43017, the HOME/COMPANY PREMISES. As previously stated in this document, MACHINE PERCEPTION is used as a mechanism to funnel money from ELEVOX to WANG and his wife BAI.

78. Furthermore, according to federalpay.org, accessed on September 23, 2021, MACHINE PERCEPTION, located at the HOME/COMPANY PREMISES, received a Coronavirus-related PPP loan from the Small Business Administration of \$15,000 in May 2020.

79. Additionally, on the State of Delaware annual franchise tax report for ELEVOX, the listed place of business was the HOME/COMPANY PREMISES.

80. As described above, WANG utilized ELEVOX and MACHINE PERCEPTION, for both of which the place of business is the HOME/COMPANY PREMISES, to profit from NIH-funded research conducted at OSU.

81. Your Affiant is also aware that the HOME/COMPANY PREMISES is the residence of WANG and BAI.

82. On or about October 20, 2021, FBI visited WANG's lab website and personal website. The websites advised that WANG and his research team utilize the 578 Dreese Laboratory, 2015 Neil Ave., Columbus, Ohio (LAB PREMISES). The website also advised that

WANG utilized 598 Dreese Laboratory, 2015 Neil Ave., Columbus, Ohio (OFFICE PREMISES) as his office.

83. WANG and his research team conducted work on NIH grants while employed at OSU. This investigation has shown that WANG has also used his research team and the research funded by NIH grants for self-profit at his companies and foreign institutions.

84. The IP addresses are further relevant to the locations listed in this Search Warrant request due to the activity that was conducted by WANG at those locations. For instance: According to information obtained from NIH, IP data from November 8, 2018 to June 8, 2021, WANG logged into NIH's system approximately 1009 times from an IP address located in Powell, Ohio, which is in the general vicinity of WANG's home address, and approximately 221 times from an IP address located at OSU in Columbus, Ohio.

85. Your Affiant is further aware from training and experience that researchers often store grant- and research-related documentation at their lab premises and office premises.

VII. ELECTRONICS

A. Terms

86. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is,

long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

B. Computers, Electronic Storage, and Forensic Analysis

87. As described above and in Attachment B, this Application seeks permission to search for records that might be found on the premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

88. *Probable cause:* I submit that if a computer or storage medium is found on the premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later

using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on actual inspection of other evidence related to this investigation, I am aware that computer equipment was used to generate, store, and/or print documents related to the allegations laid out in this Affidavit. In addition, based upon the investigation, there is reason to believe that there is a computer system currently located in or more of the SUBJECT PREMISES.

89. *Forensic evidence:* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and

movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline

information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- f. I know that when an individual uses a computer to commit crimes, or in a manner that furthers crimes, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

90. *Necessity of seizing or copying entire computers or storage media:* In most cases, a thorough search of a premises for information that might be stored on storage media requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence

of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt to do so on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

91. *Nature of examination:* Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the

warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

92. Because several people share the HOME/COMPANY PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not the direct subject of this Affidavit. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

93. In addition, the warrant Your Affiant is applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can

unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to

law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found

in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

VIII. SUMMARY

94. WANG has been employed full-time by OSU since 1991. WANG received his first NIH grant in 2012 and has continued to apply for and receive NIH funding until the time of this Affidavit.

95. WANG established or has been closely affiliated with four companies, ELEVOC, ELEVOX, MACHINE PERCEPTION, and XI'AN RESEARCH INSTITUTE. Those companies were involved in the same research WANG was conducting at OSU—research funded with NIH federal grants. WANG disclosed, untimely, and incompletely, ELEVOX to OSU. This disclosure shows that WANG had knowledge of the process to submit Conflicts of Interest. This investigation has shown that WANG has not disclosed the other companies via OSU's COI process.

96. Your Affiant is aware that, just as for renewal or revision NIH applications, initial NIH applications require NIH-funded researchers to disclose outside financial interests to their employing entity. Additionally, a Principal Investigator (the title for a project leader regarding NIH funding, of which WANG was one) has almost yearly opportunities to make these disclosures to NIH via the RPPR. Additionally, WANG had yearly opportunities to update his Conflict of Interest filing which, by design, should act as a mechanism to alert the funding agency or allow the university to mitigate a conflict. At the time of submitting new and revision applications and RPPRs, WANG had not disclosed all his outside companies, one of which was supported by a TTP contract (XI'AN RESEARCH INSTITUTE) to OSU and NIH, meaning that WANG failed to make the required disclosure to NIH of this issue.

97. Your Affiant notes further that WANG had knowledge of his obligation to make disclosures concerning conflicts of interest. Evidence of this knowledge was made apparent when OSU confronted WANG about one of his TTP affiliations and WANG provided a letter stating he was not involved with TTP any longer. With this knowledge, WANG continued to conduct activity with his talent plan work and chose not to disclose his other TTP affiliations or other companies.

98. In addition, two of WANG's companies obtained 25 patents in China related to the same narrow area of research WANG conducts for OSU. WANG has also failed to disclose to OSU and NIH that his companies have applied for 25 Chinese Patents, one of which WANG is listed as the inventor on. WANG has made materially false affirmations, via four NIH RPPRs that there have been no "inventions, patent applications and/or licenses resulted from the award during the reporting period." On or about August 31, 2016, WANG emailed OSU's Patent and Copyright Policy to his co-founder of ELEVO. This, along with the fact that WANG had filed a U.S. patent

application with OSU in 2013, shows WANG had knowledge of the process and policy to apply for patents using research conducted at OSU.

99. As described herein, the investigation has established probable cause that WANG has made material misrepresentations and omissions, in violation of 18 U.S.C. § 1001, and contrary to his ethical duties under NIH requirements and OSU policy, and that WANG has further engaged in conduct in violation of 18 U.S.C. § 1343.

100. WANG used the SUBJECT PREMISES for communications and work regarding his NIH grants, and undisclosed outside business interests.

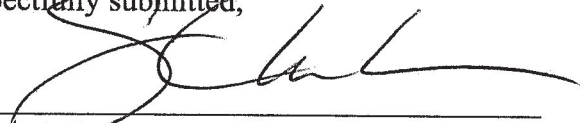
IX. CONCLUSION

101. Based on the foregoing, probable cause exists that WANG is committing one or more of the SUBJECT OFFENSES. There is probable cause to believe that evidence of those SUBJECT OFFENSES will be found at the SUBJECT PREMISES as described more fully in Attachments A-1, A-2, and A-3.

X. REQUEST FOR SEALING

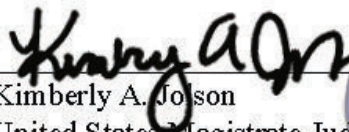
102. I further request that the Court order that all papers in support of this Application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, tamper with or destroy evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Steve McCann
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 27 day of October, 2021.



Kimberly A. Johnson
United States Magistrate Judge



ATTACHMENT A-3

The OFFICE PREMISES is located at Room 598, Dreese Laboratory, 2015 Neil Ave., Columbus, Ohio 43017.



ATTACHMENT B
Particular Things to be Seized

All records relating to the violations of the SUBJECT OFFENSES as described in this affidavit to include 18 U.S.C. § 1001 (False Statements) and 18 U.S.C. § 1343 (Wire Fraud), those violations involving Deliang WANG and any officers, directors, shareholders, employees, agents, or contractors of ELEVOC, ELEVOX, XI'AN RESEARCH INSTITUTE, and MACHINE PERCEPTION and occurring after January 1, 2015, including but not limited to:

1. Records and information related to the work being conducted by WANG related to any federally funded grants.
2. Records and information related to the patents developed by WANG or one of his companies.
3. Records and information related to the research and development of products by WANG, LENOVO, ELEVOC, ELEVOX, XI'AN RESEARCH INSTITUTE, and MACHINE PERCEPTION.
4. Records and information related to the end-users of products sold by WANG, LENOVO, ELEVOC, ELEVOX, XI'AN RESEARCH INSTITUTE, and MACHINE PERCEPTION.
5. Records and information related to the ownership or control of ELEVOC, ELEVOX, XI'AN RESEARCH INSTITUTE, and MACHINE PERCEPTION.
6. Records and information related to communications with entities or individuals in China. Your Affiant notes some records will be in Chinese and will require seizing due to lack of translation ability.
7. Records and information relating to credit card and other financial information including but not limited to bills, payment records, bank account information and records, and tax information and records.
8. Records and information related to WANG's terms of employment with OSU, including OSU policies regarding intellectual property, research funding, and conflicts of interest.
9. Records and information related to sources of funding for WANG's research, including the NIH.
10. Records and information related to any business owned, operated, or controlled to any extent by WANG, including LENOVO, ELEVOC, ELEVOX, XI'AN RESEARCH INSTITUTE, and MACHINE PERCEPTION.
11. Records and information related to any Thousand Talents Plan.
12. Records and information related to any patents related to WANG's research or the research of others associated with WANG.
13. Records and information related to WANG's research at OSU.

14. Records and information related to WANG's state of mind as it relates to the SUBJECT OFFENSES.
15. Records and information related to the involvement of any other individuals in the SUBJECT OFFENSES.
16. Records and information related to WANG's foreign/domestic financial accounts, holdings, and relationships.
17. Records and information related to meetings or communications concerning WANG's companies and research collaborations at Northwestern Polytechnical University.
18. Records and information related to any financial transaction or other movement of any things of value, to or from WANG, as well as any documents, including but not limited to Forms 1099 and Forms W-2, filed with any taxing authority in connection with those transactions.
19. Records and information related to any financial transaction or other movement of any things of value, to or from any company with which WANG is affiliated, as well as any documents, including but not limited to Forms 1099 and Forms W-2, filed with any taxing authority in connection with those transactions.
20. Computers and/or storage media related to the allegations laid out in this Affidavit. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - i. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - ii. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - iii. evidence of the lack of such malicious software;
 - iv. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - v. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - vi. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - viii. evidence of the times the COMPUTER was used;
 - ix. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- x. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- xi. records of or information about Internet Protocol addresses used by the COMPUTER;
- xii. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- xiii. contextual information necessary to understand the evidence described in this attachment.
- xiv. Routers, modems, and network equipment used to connect computers to the Internet.
- xv. WANG's biometrics, such as fingerprints or facial recognition, may be used to unlock any computer.

21. Additional terms:

- i. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
- ii. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.
- iii. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.